

1 WO

2  
3  
4 **IN THE UNITED STATES DISTRICT COURT**  
5 **FOR THE DISTRICT OF ARIZONA**  
6

7 United States of America,

8 Plaintiff,

9 v.

10 Michael Anthony Williams - 005,  
11 Samuel Lee Berrelle Rakestraw, III – 004,  
12 Shawmaine Eustace Ardell Moore – 003,

13 Defendants.  
14

CR-18-01695-TUC-JAS (EJM)

**REPORT AND  
RECOMMENDATION**

15 Pending before the Court is a Motion to Suppress Cell Phone Records filed by  
16 defendants Michael Anthony Williams ("Williams"), Samuel Berrelle Rakestraw  
17 ("Rakestraw"), and Shawmaine Eustace Ardell Moore ("Moore"). (Doc. 1149.) They  
18 argue that the government's acquisition of cell site records was unconstitutional because  
19 they used a court order under 18 U.S.C. § 2703(c) to obtain that information, rather than a  
20 search warrant as required by *Carpenter v. United States*, 138 S.Ct. 2206 (2018). The  
21 government concedes that *Carpenter* now requires a search warrant to obtain cell site  
22 information. However, the government points out that it obtained the cell site information  
23 in 2015, three years before *Carpenter*, when a court order was all the law required. (Doc.  
24 1192.) As a result, the government argues that the "good-faith" exception applies, and  
25 therefore, the defendant's motion should be denied. For the reasons that follow, the Court  
26 concludes that the good faith exception does not apply to the unique factual situation in the  
27 case at hand, and therefore, recommends that the District Court grant the Motion to  
28 Suppress.

1 **FACTUAL BACKGROUND**

2 The charges against the defendants have been detailed in several Orders and Reports  
3 and Recommendations addressing other motions, and the specific charges are not relevant  
4 to the instant motion. In summary, all three defendants are charged with a RICO  
5 conspiracy, the objects of which are murder, violent acts, drug trafficking, and obstruction  
6 of justice. The defendants are also charged with murder and violent acts in aid of  
7 racketeering. Williams is also charged with drug trafficking conspiracies, substantive drug  
8 trafficking offenses, and prohibited possessor offenses.

9 **A. The Petitions for Cell Site Information and the State Judge's Orders.**

10 On July 22, 2015, Tucson Police Detective Vance Padilla filed two petitions with a  
11 Pima County Superior Court Judge which sought orders to obtain certain phone records  
12 relating to the defendants. (Gov. Exs. 1 and 2.) Specifically, the petitions requested  
13 subscriber information, call detail records, and cellular tower utilization information (*i.e.*,  
14 cell site information, cell site locations, and location information). *Id.* at 202670, 202724.  
15 Detective Padilla provided a fairly detailed account of the background of his investigation  
16 and why the requested records were relevant to and would further the investigation.  
17 However, Detective Padilla did not cite to the (federal or state) statutory authority that  
18 would permit the state court judge to issue orders for the information requested. He also  
19 did not request that notice to the subscribers of law enforcement's request for this  
20 information be delayed. *See* 18 U.S.C. § 2705.

21 The state judge granted the petitions and issued two orders directing Metro PCS and  
22 T-Mobile to provide the requested information. *Id.* at 202681, 202735. The judge  
23 referenced 18 U.S.C. § 2703 (but not the specific subsection) as the basis for each order,  
24 even though that statute was not mentioned in the petitions. Each order also includes a  
25 nondisclosure provision directed at the service providers which reads as follows:

26  
27 Due to the sensitivity of this on-going criminal investigation, the notification  
28 to the listed subscribers by [the cell phone company] that these records have  
been released to a law enforcement agency could compromise this  
investigation as well as the safety of law enforcement officers participating

1 in the investigation. Based on these facts, it is further ordered that the  
 2 customer/subscriber is not to be notified of the release of this information, as  
 it could jeopardize an on-going criminal investigation.

3 *Id.* at 202683, 202737.

4 The orders do not include a provision authorizing law enforcement to delay notice  
 5 to the subscribers or customers that their cell site information is being obtained.

6 **B. The Motion to Suppress Cell Site Records.**

7 On February 2, 2022, defendants Williams, Rakestraw, and Moore filed a Motion  
 8 to Suppress Cell Phone Records. They argue that to obtain historical cell site information,  
 9 which essentially tracked their movements when they had their phones, Detective Padilla  
 10 was required to obtain a search warrant. The defendants rely on *Carpenter* where the  
 11 Supreme Court held just that. The government points out the instant petitions were filed  
 12 in 2015, three years before *Carpenter* was decided. The government argues that pre-  
 13 *Carpenter*, law enforcement routinely and lawfully utilized 18 U.S.C. §§ 2703(c) and  
 14 2703(d) to obtain historical cell site information. As such, the government maintains that  
 15 it complied with the Stored Communications Act (SCA) which was lawful in 2015, and  
 16 therefore, the good-faith exception articulated by the Ninth Circuit in *United States v.*  
 17 *Korte*, 918 F.3d 750 (9<sup>th</sup> Cir. 2019), applies and suppression of the cell site records is not  
 18 warranted.

19 **1. Detective Padilla's Testimony.**

20 On March 14, 2022, the Court held an evidentiary hearing on the motion to suppress.  
 21 Detective Padilla testified as follows on direct examination about his petitions to acquire  
 22 cell site information. Detective Padilla has been employed with the Tucson Police  
 23 Department ("TPD") since 2001 and was promoted to the rank of detective in 2009. Tr.  
 24 3/14/22 (Doc. 1331) at 13. He was assigned to the gang unit in 2010. *Id.* On July 22,  
 25 2015, Detective Padilla submitted two petitions to a state court judge that requested  
 26 historical cell site information for the defendants' cellular phones. *Id.* at 14; Gov. Exs. 1  
 27 and 2. He testified that, at that time, his understanding of the process for obtaining cell  
 28

1 site information was obtaining a court order which was based on probable cause. Tr.  
2 3/14/22 at 14. That is why he included a probable cause statement in his petitions. *Id.* at  
3 16.

4 Government counsel asked how Detective Padilla knew it was “standard practice”  
5 at that time to obtain a court order for cell site information. He testified as follows:

6 In working with a company named the Phoenix Training Council and then  
7 which turned into ZetX, they provided services and templates for court orders  
8 to acquire search warrants and court orders for phone records and it was the  
9 standard that the detectives in our department were obtaining records so it  
was just – it was like the everyday practice that was being done at the time.

10 *Id.* at 15.

11 He was given that direction by his superiors at TPD, and never had an indication  
12 that he was supposed to obtain a search warrant for cell site information. *Id.* He had no  
13 knowledge of any pending court cases where challenges were being made to acquiring cell  
14 site information by a court order. *Id.* at 15-16.

15 On cross-examination, Detective Padilla testified that a company named ZetX  
16 “would provide templates for the different service providers where you would fill in your  
17 probable cause and specifics related to whatever case you were working.” *Id.* at 19.  
18 Detective Padilla testified that he did not obtain a search warrant because a court order was  
19 “the standard at the time.” *Id.* at 23.

20 Detective Padilla filled out the petitions as well as the orders that he submitted to  
21 the state judge. *Id.* Detective Padilla acknowledged that his report reflects that the state  
22 judge asked him questions and he answered the questions, but he does not recall the  
23 conversation. *Id.* at 27. He conceded that it is possible the state judge could have asked  
24 him why he was not requesting a search warrant. *Id.* at 28. He also conceded that in 2015  
25 there were federal agents involved in the investigation; however, law enforcement did not  
26 then know if this would become a federal investigation and “come to federal court[.]” *Id.*  
27 at 28-29. Detective Padilla has never obtained a federal search warrant, so he is not  
28 familiar with the process. *Id.* at 29.

1 On redirect examination, Detective Padilla testified that he did not “know the big  
2 difference” between obtaining a court order or a search warrant for cell site information.  
3 *Id.* at 31. But if the standard was to obtain a search warrant, he would have obtained a  
4 warrant. *Id.* However, in 2015 no one had “given any indication that these petitions were  
5 not the appropriate way to get historical cell site records.” *Id.* at 32.

6 As a result of questions asked of counsel by the Court, Detective Padilla was  
7 recalled. He again testified that he drafted the court orders for the state judge, and they  
8 were submitted at the same time as the petitions. *Id.* at 36. The Court asked Detective  
9 Padilla to explain why he did not cite the statute that provides the legal basis to obtain the  
10 requested information. *Id.* at 36-37. Detective Padilla testified that at the time, officers  
11 used “standard templates,” so these petitions had been created using “a standard template  
12 that was brought or presented by the ZetX company to elicit what we needed.” *Id.* at 37.  
13 Detective Padilla explained that the companies that he was seeking the cell site information  
14 from provided him with what the companies needed in the petitions and the orders to  
15 provide the requested information. *Id.* The company drafted the templates for the petitions  
16 and orders, and officers would download it from their website, fill it out, and “then print it  
17 as our final product and that would be presented to the judge.” *Id.* at 37-38.

## 18 **2. Oral Arguments and Supplemental Pleadings.**

19  
20 Following Detective Padilla’s testimony, the Court held oral argument on the instant  
21 motion. The Court pointed counsel to the following provision contained in 18 U.S.C. §  
22 2703(d): “In the case of a State governmental authority, such a court order shall not issue  
23 if prohibited by the law of such State.” The Court questioned whether there was an  
24 equivalent state statute to 18 U.S.C. § 2703 which authorized the acquisition of cell site  
25 information, and if so, whether that statute was either more restrictive than Section 2703  
26 or provided additional procedural safeguards than Section 2703. If that is the case and the  
27 government acquired cell site information in a manner prohibited by state law, then it  
28 arguably did not comply with the SCA and cannot rely on the good-faith exception. The

1 parties suggested submitting supplemental pleadings on this provision.

2 In their supplemental pleading, the defense argued that A.R.S. § 13-3016 is the state  
3 equivalent to Section 2703(c) and that state statute is more restrictive than Section 2703(c)  
4 because A.R.S. § 13-3016 requires that prior notice be provided to the subscriber or  
5 customer before cell site information may be obtained unless the court orders that notice  
6 be delayed. The defense points out that notice was never provided or ordered delayed as  
7 required by A.R.S. § 13-3016. The defense contends that because the government did not  
8 comply with the more restrictive state law as required by Section 2703(d), the government  
9 did not comply with the SCA, and the good-faith exception does not apply.

10 In their supplemental pleading, the government asserted that A.R.S. § 13-3017 is  
11 the state equivalent to Section 2703(c) and this statute provides that cell site records may  
12 be obtained by an *ex parte* court order without notice to the subscriber or customer. And  
13 A.R.S. § 13-3017 only requires a certification that the information likely to be obtained by  
14 a pen register or trap and trace device is relevant to an ongoing investigation. Because both  
15 the petitions for cell site information and the state court's orders authorizing the production  
16 of that information complied with state law and the SCA, the good-faith exception applies  
17 and defeats the motion to suppress.

18 The Court held another oral argument on March 17, 2022, to address the  
19 supplemental pleadings. The Court noted that A.R.S. § 13-3017 does not appear to be the  
20 Arizona statutory equivalent to Section 2703(c), but rather the equivalent to the federal  
21 pen/trap statute. *See* 18 U.S.C. § 3121, *et. seq.* As a result, the government filed a second  
22 supplemental pleading in which it claimed that A.R.S. § 13-3018 is also the state law  
23 equivalent to Section 2703(c). The government maintains that, at least in 2015, A.R.S. §  
24 13-3018 allowed the state to obtain cell site information with a subpoena. Thus, they claim  
25 that state law was not violated because Detective Padilla did more than state law required  
26 by obtaining court orders.

27 In response, the defense filed a second supplemental pleading to address A.R.S. §  
28 13-3018. The defense argues that neither the plain language of this statute nor the Arizona

1 Supreme Court case that the government cites support their position that section 13-3018  
 2 applies to cell site information. To the contrary, the defense asserts that the Arizona  
 3 Supreme Court has made clear that A.R.S. § 13-3016 applies to requests for and orders  
 4 requiring the production of cell site information.

## 5 **DISCUSSION**

### 6 **A. The Stored Communications Act Pre-Carpenter.**

7  
 8 The Stored Communications Act (“SCA”) allows the government to obtain stored  
 9 electronic communication information from electronic communication service providers.  
 10 See 18 U.S.C § 2701, *et seq.* As set forth below, the legal mechanism by which the  
 11 government can obtain electronic communication information pursuant to the SCA turns  
 12 on whether the government is seeking the content of electronic communications or non-  
 13 content records related to electronic communications. The SCA then imposes legal  
 14 requirements on the government based on the mechanism utilized.

15 Section 2703(a) applies to requests for the contents of electronic communications  
 16 in storage less than 180 days. Those communications can only be obtained by a search  
 17 warrant. That subsection does not require prior notice to the customer or subscriber before  
 18 obtaining the communications. 18 U.S.C. § 2703(a).

19 Section 2703(b) applies to requests for the contents of electronic communications  
 20 in storage for more than 180 days. The request for those communications can be made in  
 21 three ways. The government may seek a search warrant, which again does not require prior  
 22 notice to the subscriber or customer. 18 U.S.C. § 2703(b)(1)(A). Alternatively, the  
 23 government can seek to obtain those communications by subpoena or a Section 2703(d)  
 24 court order, provided that prior notice is provided by the government to the customer or  
 25 subscriber. 18 U.S.C. § 2703(b)(1)(B). That said, notice to the subscriber or customer can  
 26 be delayed by a court for up to 90 days at the government’s request pursuant to 18 U.S.C.  
 27 § 2705. That section also allows a court, upon the government’s request, to extend the  
 28



1 required notice for additional 90-day periods. *Id.*<sup>1</sup>

2 Section 2703(c), titled “Records Concerning Electronic Communication Service or  
3 Remote Computing Service,” provides that the government may request the records  
4 pertaining to a “record or other information pertaining to a subscriber or customer” from  
5 the provider of an electronic communication service or remote computing service. 18  
6 U.S.C. § 2703(c). Although it is not clear from the plain language of this subsection,  
7 Section 2703(c) has been interpreted by federal courts to include requests for cell site  
8 information. Section 2703(c) provides that the government may obtain this information by  
9 a search warrant or a Section 2703(d) court order (as well as other means not implicated in  
10 the case at hand). When records are sought by a search warrant or pursuant to a court order  
11 based on Section 2703(c), the government does not have to provide any notice, let alone  
12 prior notice, to the subscriber or customer. 18 U.S.C § 2703(c)(3).

13 To obtain a court order pursuant to Section 2703(d) for electronic communications  
14 covered by Section 2703(c), the government must “offer[] specific and articulable facts  
15 showing that there are reasonable grounds to believe that. . .the records or other information  
16 sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. §  
17 2703(d). Section 2703(d) further provides that “[i]n the case of a State governmental  
18 authority, such a court order shall not issue if prohibited by the law of such State.” As  
19 will become evident, the instant motion turns on this sentence.

20 The SCA expressly rules out exclusion of evidence as a remedy for a violation. *See*  
21 *United States v. Smith*, 155 F.3d 1051, 1056 (9<sup>th</sup> Cir. 1998) (unlike the Wiretap statute, the  
22 Stored Communications Act does not provide an exclusion remedy). The SCA only allows  
23 for civil damages and criminal punishment. *See* 18 U.S.C. §§ 2701(b) and 2707. However,  
24 the SCA’s limitation of remedies only applies to non-constitutional challenges to the

---

25  
26 <sup>1</sup> The Court notes that Section 2703(b) is clearly unconstitutional as a result of *Carpenter*’s  
27 holding that a search warrant is required to obtain cell site information, which is much less  
28 intrusive than obtaining content. In any event, Section 2703(b) is not relevant to the issue  
at hand.



1 acquisition of information pursuant to the SCA.

2 **B. The State Judge’s Section 2703(d) Order Was Issued Pursuant to**  
 3 **18 U.S.C. § 2703(c).**

4 As mentioned earlier, Detective Padilla’s petitions submitted to the state judge do  
 5 not reference 18 U.S.C. § 2703, let alone a subsection of that statute. The state judge’s  
 6 orders reference 18 U.S.C. § 2703, but not a specific subsection of the statute.  
 7 Notwithstanding any indication of the specific subsection of the SCA that was used to  
 8 request the cell site information, or the orders that directed the production of that  
 9 information, this Court finds that, based on a process of elimination, the petitions for cell  
 10 site information had to have been based on Section 2703(c). As discussed above, Section  
 11 2703(a) and Section 2703(b) both pertain to the “[c]ontents of wire or electronic  
 12 communications.” By contrast, Section 2703(c) pertains to “[r]ecords concerning  
 13 electronic communication.” Thus, because the cell site data is not the “content of  
 14 communications,” Section 2703(c) was the statutory basis for the petitions and the resultant  
 15 orders. As a result, Section 2703(c) did not require the government to provide notice, let  
 16 alone prior notice, to the defendants about the government’s receipt of records relating to  
 17 their phone records. 18 U.S.C. § 2703(c)(3).

18 In order to obtain a Section 2703(d) court order for cell site information based on  
 19 Section 2703(c), the government had to “offer[] specific and articulable facts showing that  
 20 there are reasonable grounds to believe that . . . the records or other information sought,  
 21 are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).  
 22 Detective Padilla’s petition submitted to the state court in 2015 clearly met that standard,  
 23 which is less exacting than the probable cause required for a search warrant. However, as  
 24 discussed below, the law changed dramatically three years later.

25 **C. Challenges to the Stored Communications Act Post-Carpenter.**

26 In *Carpenter*, the Supreme Court held that a search warrant was required to obtain  
 27 cell site information. That decision was a substantial change in the law because the  
 28 government routinely used an 18 U.S.C. § 2703(d) court order to obtain that information.

1 As a result, *Carpenter* produced many challenges to Section 2703(d) orders issued prior to  
2 *Carpenter* that were used to obtain cell site information. Not surprisingly, the government  
3 has relied on the “good-faith” exception articulated by the Supreme Court in *Illinois v.*  
4 *Krill*, 480 U.S. 340 (1987), to defend against *Carpenter* challenges to the acquisition of  
5 cell site information by a Section 2703(d) order.

6 In *United States v. Korte*, 918 F.3d 750 (9<sup>th</sup> Cir. 2019), the Ninth Circuit applied the  
7 good-faith exception to requests for historical cell tower data made to third parties under  
8 the Stored Communications Act. Specifically, that court held that cell tower data  
9 information “acquired pre-*Carpenter* is admissible – so long as the government satisfied  
10 the SCA’s then-lawful requirements – under [the Supreme Court’s] good-faith exception.”  
11 *Korte*, 918 F.3d at 759.

12 In light of *Korte*, to rely on the good faith exception the government must have  
13 satisfied the SCA’s then-lawful requirements, meaning that the government jumped  
14 through every hoop set forth in the SCA to obtain an order for cell site information. For  
15 the reasons detailed below, the Court concludes that the government did not satisfy the  
16 requirements of the SCA. As a result, the good faith exception does not apply and  
17 suppression of the cell site information is warranted.

18 **D. The Good-Faith Exception Turns on Arizona Law.**

19 The government argues that the defendants’ suppression argument is blown out of  
20 the water by *Korte* because it satisfied the SCA’s then-lawful requirements to obtain the  
21 cell site information. Specifically, it obtained Section 2703(d) court orders to acquire the  
22 cell site information, which is all that the law required in 2015. The defense maintains that  
23 the government did not comply with the SCA because the manner in which they obtained  
24 the cell site information – *i.e.*, without providing notice to the subscriber or customer or  
25 obtained delayed notice from the state court – is prohibited under Arizona State law. And  
26 Section 2703(d) mandates that an order can only issue under that statute if not prohibited  
27 by state law.  
28

1 At first blush, it seems apparent that both the government's requests for a Section  
2 2703(d) order for cell site information and the resultant orders complied with the SCA.  
3 However, state law indeed creeps into that analysis based on the following provision  
4 contained in Section 2703(d): "In the case of a State governmental authority, such a court  
5 order shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Because  
6 Detective Padilla is a state law enforcement officer, for purposes of the good faith  
7 exception, the Court must determine whether the government acquired cell site information  
8 in a manner prohibited by state law.

9 To make that determination, the Court must examine both the plain language of  
10 three Arizona statutes that the parties contend support their respective positions regarding  
11 the equivalent Arizona State Statute to Section 2703(c), and three Arizona State cases that  
12 address each statute. As will become evident, it is difficult to discern from the plain  
13 language of the state statutes which statute applies to applications and orders for cell site  
14 information. As such, that issue must be primarily resolved by the few Arizona cases that  
15 address these statutes.

16 **1. A.R.S. Section 13-3017 and Conner.**

17 A.R.S. § 13-3017 is titled: "Ex parte order for pen register or trap and trace device."  
18 This statute allows for a prosecutor or law enforcement officer to apply to a state court "for  
19 an ex parte order authorizing the installation and use of a pen register or a trap and trace  
20 device." A.R.S. § 13-3017(A). The application must be made in writing and under oath,  
21 and detail the following information: (1) the name and title of the applicant; (2) the phone  
22 number or other identifier; the identity of the subscriber (if known); the location of the  
23 telephone line or other facility that the pen register or trap and trace device is to be attached  
24 to; and the geographic limits of the order; (3) a certification that the information to be  
25 obtained is relevant to an ongoing criminal investigation; and (4) a statement of the offense  
26 to which the information likely to be obtained by the device relates. A.R.S. § 13-  
27 3017(A)(1)-(4). The statute provides that the judge shall issue an ex parte order if the judge  
28 finds that the applicant has complied with the requirements set forth above. A.R.S. § 13-

1 3017(B).

2 In *State v. Conner*, 249 Ariz. 121 (App. Div. 1 2020), the court cited to A.R.S. § 13-  
3 3017, but provided no substantive discussion of that statute. In that case, the police  
4 requested and obtained an ex parte court order to obtain the defendant's cell phone records.  
5 249 Ariz. at 122. The court noted that the request was made pursuant to A.R.S. § 13-3017  
6 and 18 U.S.C. § 2703. *Id.* The court found that the request was supported by probable  
7 cause and issued an order that directed the cell phone provider to supply certain records,  
8 including cell site information. *Id.* The defendant moved to suppress the cell site location  
9 information based on *Carpenter* because a search warrant (based on a finding of probable  
10 cause) was not used to obtain that information. *Id.* The trial court denied the motion noting  
11 that the application and court order were based on probable cause, and the order was the  
12 functional equivalent of a warrant. *Id.* at 123-124.

13 On appeal, the defendant argued that the court order was not supported by probable  
14 cause because it was issued pursuant to the SCA (*i.e.*, 18 U.S.C. § 2703), which *Carpenter*  
15 found was a “gigantic” departure from the probable cause rule. *Id.* at 250. The defendant  
16 pointed out that Section 2703 only requires “reasonable grounds” and not probable cause  
17 for the issuance of an order for cell site information. *Id.* “Because Arizona’s statute  
18 requires a similar showing as its federal counterpart,” the defendant argued that “if 18  
19 U.S.C. § 2703 falls below the probable cause rule, then so does A.R.S. § 13-3017.” *Id.*

20 The Court of Appeals first noted that the defendant’s argument was based on the  
21 false premise “that the request was not based on probable cause, and that the order was not  
22 issued on a probable cause finding.” *Id.* The court essentially concluded that the order  
23 was the functional equivalent of a search warrant because the request for the order was  
24 based on probable cause and the order was issued based on a finding of probable cause. *Id.*  
25 For that reason, the Court affirmed the denial of the suppression motion on this ground.  
26 *Id.* at 125-126.

27 The government relies on *Conner* to support its argument that A.R.S. § 13-3017 is  
28 the state equivalent to 18 U.S.C. § 2703(c) for obtaining cell site information. The

1 government reasons that A.R.S. § 13-3017, just like Section 2703(c), does not require that  
2 notice be provided to the subscriber or customer. As a result, Arizona law does not prohibit  
3 the acquisition of cell site information unless prior notice is provided to the customer or  
4 subscriber. And since no notice is required under A.R.S. § 13-3017 or Section 2703(c), no  
5 delayed notice requests were necessary.

6 The defense argues that *Conner* does not support the government's argument that  
7 A.R.S. § 13-3017 authorizes the production of cell site information, and even if it did, the  
8 Arizona Supreme Court in *State v. Smith*, 250 Ariz. 69 (2020), later made clear that A.R.S.  
9 § 13-3016 authorizes the state to obtain cell site information. Additionally, Detective  
10 Padilla's petitions do not cite any statute, let alone A.R.S. § 13-3017, and the petitions and  
11 state judge's orders never use the language in A.R.S. § 13-3017.<sup>2</sup>

12 The Court disagrees with the government's interpretation of both A.R.S. § 13-3017  
13 and *Conner*. A.R.S. § 13-2017 is clearly not the state law equivalent to Section 2703(c).  
14 Rather, A.R.S. § 13-3017 is the Arizona pen/trap statute, which is the state equivalent to  
15 18 U.S.C. § 3122. Pen/trap information is prospective and real time data, but the data is  
16 limited to the phone numbers used to make and receive calls or text messages. By contrast,  
17 cell site information is historical data that includes where a phone was located when a call  
18 or text message was made or received, in addition to the phone numbers of the calls made  
19 and received. Thus, it is clear that neither the federal nor Arizona State pen/trap statute  
20 can be used to obtain cell site information.

21 The Court notes that the government's reliance on *Conner* appears to be based on  
22 two references to A.R.S. § 13-3017 in that opinion. This Court does not glean much from  
23 these references. The first reference is when the Court notes that the government applied  
24 for the order under A.R.S. § 13-3017 and Section 2703. This Court believes that the State  
25 requested pen/trap information under A.R.S. § 13-3017, as well as historical cell site

---

26 <sup>2</sup> The defense notes that in their second supplemental pleading, the government seems to  
27 abandon its argument that A.R.S. § 13-3017, the Arizona pen/trap statute, authorizes the  
28 production of cell site information by an ex parte court order and does not require notice  
to the subscriber or customer. Instead, the government now contends that Section 13-3018  
is the equivalent Arizona statute to Section 2703(c).

1 information under Section 2703. There was simply no reason to cite both statutes to request  
 2 cell site information. In fact, the federal pen/trap statute exists in conjunction with Section  
 3 2703(c), and dual requests for pen/trap information and requests for court orders for cell  
 4 site information pursuant to Section 2703(c) were routinely made to Magistrate Judges in  
 5 this District prior to *Carpenter*.

6 The second reference by the *Conner* court to A.R.S. § 13-3017 is when the  
 7 defendant in that case made the argument noted above about A.R.S. § 13-3017 and Section  
 8 2703 both falling below the probable cause rule. However, the Court of Appeals did not  
 9 address that argument or provide any substantive discussion about the applicability of  
 10 A.R.S. § 13-3017 to requests for cell site information (or pen/trap information). And the  
 11 Court's affirmance of the denial of the motion to suppress did not turn on a comparison of  
 12 A.R.S. § 13-3107 and Section 2703, or the legal requirements for utilizing either statute to  
 13 obtain cell site records. Rather, the Court found that the order was the functional equivalent  
 14 of a warrant because it was supported by probable cause. The precedential value of *Conner*  
 15 is that finding. And, as discussed below, the precedential value of *Conner* with respect to  
 16 that finding has been called into question by the Arizona Supreme Court in *Smith*.

## 17 **2. A.R.S. Section 13-3018 and *Mixton*.**

18 A.R.S. § 13-3018 is titled: "Communication service records; subpoenas,  
 19 application; certification; definition." This section applies to all communication service  
 20 providers that do business in Arizona or furnish communication services to persons in  
 21 Arizona. A.R.S. § 13-3018(A). To obtain communication service records covered by this  
 22 statute, a prosecutor may issue a subpoena duces tecum or grand jury subpoena to a  
 23 communication service provider for information needed in a criminal investigation or  
 24 prosecution. A.R.S. § 13-3018(B). The prosecutor who issues the subpoena must "certify  
 25 in the body of the subpoena that the information likely to be obtained is relevant to an  
 26 ongoing criminal investigation." A.R.S. § 13-3018(C). "Communication service records"  
 27 for purposes of this statute includes:

28 [S]ubscriber information, including name, billing or installation address,  
 length of service, payment method, telephone number, electronic account

1 identification and associated screen names, toll bills or access logs, records  
 2 of the path of an electronic communication between the point of origin and  
 3 the point of delivery and the nature of the communication service provided,  
 4 such as caller identification, automatic number identification, voice mail,  
 electronic mail, paging or other service features. Communication service  
 records do not include the content of any stored oral, wire, or electronic  
 communication.

5 A.R.S. § 13-3018(G).

6 In *State v. Mixton*, 250 Ariz. 282, 297 (2021), the Arizona Supreme Court made  
 7 multiple references to A.R.S. § 13-3018, but the court did not address this statute's  
 8 applicability to requests and orders for cell site information. In that case, the Arizona  
 9 Supreme Court was presented with the issue of whether the Fourth Amendment (or the  
 10 Arizona State Constitution) required a search warrant to be obtained for internet protocol  
 11 (IP) addresses or subscriber information. 250 Ariz. at 285. The defense was asking the  
 12 court to expand *Carpenter's* reach to encompass not only requests for cell site information,  
 13 but also IP address and subscriber information. *Id.* In refusing to do so, the Court noted  
 14 that subscriber information and IP addresses "do not reveal the substance or content of the  
 15 internet user's communication any more than the information affixed to the exterior of a  
 16 mailed item." *Id.* at 287. The Court also noted that the nature of an IP address and  
 17 subscriber information is fundamentally different from cell site data's "perpetual  
 18 surveillance attributes." *Id.* at 288. The Court cited A.R.S. § 13-3018 several times in  
 19 noting that this statute authorizes law enforcement to use subpoenas to obtain subscriber  
 20 and other non-content service provider information records.

21 The government maintains that *Mixton* makes clear that A.R.S. § 13-3018 applies  
 22 to requests for cell site information, and therefore, is also a state court equivalent to Section  
 23 2703(c). The government points out that the Arizona Supreme Court held that "[t]he  
 24 Arizona legislature has authorized the state to issue administrative subpoenas for subscriber  
 25 information and **other non-content service provider records** based on a showing that the  
 26 information likely to be obtained is relevant to an ongoing criminal investigation." (Doc.  
 27 1317 at 6; emphasis in original.)

28 The government also argues that A.R.S. § 13-3018(G), the definitional subsection



1 of Section 13-3018, authorizes the production of cell site information because that  
2 subsection refers to “records of the path of an electronic communication between the point  
3 of origin and the point of delivery.” And that subsection further provides that  
4 “[c]ommunication service records do not include the content of any stored oral, wire or  
5 electronic communication.” A.R.S. § 13-3018(G). The government asserts that by  
6 obtaining a court order for cell site information, Detective Padilla did more than was  
7 required under Section 13-3018. Because Detective Padilla complied with the then-lawful  
8 Arizona statutory equivalent to Section 2703(c), the government reasons that the good-  
9 faith exception applies, and the suppression motion is without merit.

10 The defense first argues that A.R.S. § 13-3018 "does not apply to law enforcement,  
11 but to prosecutors." As a result, "Detective Padilla could not utilize this section even if he  
12 wanted to." (Doc. 1324 at 3.) Additionally, the defense argues that a finding that A.R.S.  
13 § 13-3018 applies to cell site requests would depart from *Carpenter*'s holding that a search  
14 warrant setting forth probable cause is required to obtain cell site information, and a court  
15 order based on “reasonable grounds” is insufficient. The defense further argues that the  
16 government's reliance on *Mixon* “completely ignores the Arizona Supreme Court's  
17 reliance on *Carpenter* in holding that IP addresses and ISP subscriber information (not at  
18 issue here) was not within the same privacy interest as CSLI records.” *Id.* at 4. The defense  
19 maintains that *Mixon* demonstrates that a subpoena would not be the vehicle to obtain cell  
20 site information. Finally, the defense argues that the Arizona Supreme Court in *State v.*  
21 *Smith*, 250 Ariz. 69 (2020), made clear that A.R.S. § 13-3016 applies to the acquisition of  
22 cell site information, and not A.R.S. § 13-3018.

23 The Court finds that *Mixon* is not helpful to the analysis of whether A.R.S. § 13-  
24 3018 applies to requests and orders for cell site information. The Arizona Supreme Court's  
25 “references” to A.R.S. § 13-3018 shed no light on that issue. First, that Court was not  
26 dealing with the good-faith exception's applicability to a *Carpenter* violation. Second, the  
27 Court was not dealing with a request for cell site information under A.R.S. § 13-3018. In  
28 fact, the request for subscriber information and IP addresses was made via a federal

1 administrative subpoena, not A.R.S. § 13-3018. Third, the court noted that IP addresses  
 2 and "subscriber information is fundamentally different from CSLI's perpetual surveillance  
 3 attributes." *Mixon*, 250 Ariz. at 288. As a result, the Court never addressed or even  
 4 touched on whether, prior to *Carpenter*, A.R.S. § 13-3018 allowed cell site information to  
 5 be obtained by use of a subpoena. Therefore, *Mixon*, does not support the government's  
 6 argument that A.R.S. § 13-3018 is the state law equivalent to Section 2703(c).

### 7 **3. A.R.S. Section 13-3016 and Smith.**

8 A.R.S. § 13-3016 is titled: "Stored oral, wire and electronic communications;  
 9 agency access; backup preservation; delayed notice; records preservation request;  
 10 violation; classification." A.R.S. § 13-3016 "applies to oral, wire and electronic  
 11 communications that are entrusted to a communication service provider or remote  
 12 computing service solely for the purpose of transmission, storage or processing." A.R.S.  
 13 § 13-3016(A). The state "may require the disclosure" of records "by a communication  
 14 service provider or remote computing service of the contents of an oral, wire or electronic  
 15 communication" that is in electronic storage in three ways: (1) without prior notice to the  
 16 subscriber or party by obtaining a search warrant; (2) with prior notice to the subscriber or  
 17 party, by serving a subpoena, except notice may be delayed pursuant to subsection (D); or  
 18 (3) with prior notice to the subscriber or party (which again can be delayed under  
 19 subsection (D)), "by obtaining a court order on an application and certification that contains  
 20 specific and articulable facts showing that there are reasonable grounds to believe that the  
 21 communication content sought is relevant to an ongoing criminal investigation." A.R.S. §  
 22 13-3016(B)(1)-(3).<sup>3</sup>

23 The notice to the subscriber or party that is required by Section 13-3016 "may be  
 24 delayed for a period of not to exceed ninety days" if the applicant for a search warrant or  
 25 court order "requests a delay of notification and the court finds that delay is necessary to

---

26 <sup>3</sup> The Court notes that subsection (B) states that it applies to records in electronic storage  
 27 for less than 180 days, and subsection (C) states that it applies to records in electronic  
 28 storage for more than 180 days. However, the legal processes to obtain this information is  
 identical regardless of the length of time the records have been in electronic storage. As  
 such, it is not apparent why this statute makes this time distinction.

1 protect the safety of any person or to prevent flight from prosecution, tampering with  
2 evidence, intimidation of witnesses or jeopardizing an investigation." A.R.S. § 13-  
3 3016(D)(1). "If further delay of notification is necessary, extensions of up to ninety days  
4 each may be obtained by application to the court.... " A.R.S. § 13-3016(E).<sup>4</sup> A.R.S. § 13-  
5 3016(G) provides that upon expiration of the delayed notice, "the agency shall deliver to  
6 the subscriber or party a copy of the process used and notice" including: (1) that  
7 information was requested by the service provider; (2) the date the information was  
8 requested; (3) that notification was delayed; (4) the identity of the court or agency ordering  
9 or certifying the delay; (5) the provision by which the delay was obtained; and (6) that any  
10 challenge to the subpoena or order must be filed within 14 days.

11 In *Smith*, the Arizona Supreme Court directly addressed Section 13-3016's  
12 applicability to requests and orders for historical cell site information. In that case, on  
13 September 13, 2016, the State obtained the defendant's cell site information by a court  
14 order pursuant to A.R.S. § 13-3016. *Smith*, 250 Ariz. at 80. The service provider did not  
15 provide the contents of any communications. *Id.* The defendant moved to suppress the  
16 cell site information, arguing that under *Carpenter* (apparently decided between the  
17 indictment and trial), the State could not obtain his cell site information without a search  
18 warrant supported by probable cause. *Id.* Additionally, the defendant argued that the State  
19 violated A.R.S. § 13-3016 by failing to provide him with notice of the cell site order. *Id.*  
20 The trial court denied the suppression motion, concluding that (1) there was probable cause  
21 to support the cell site order; and (2) lack of notification under A.R.S. § 13-3016 was not  
22 grounds for suppression of the cell site information. *Id.*

23 On appeal, the defendant argued that because the State did not obtain a search  
24 warrant, it did not comply with *Carpenter* and the cell site information should have been  
25 suppressed. *Id.* The State conceded that under *Carpenter* a search warrant was required

---

26 <sup>4</sup> Upon application, the court can issue what is commonly referred to as a "gag order,"  
27 which prohibits the communication service provider from notifying the customer or  
28 subscriber of the search warrant, court order, or subpoena, if the court finds that notice may  
cause an adverse result described in subsection (D). A.R.S. § 13-3016(F). The order  
prohibiting notification by the communication service provider can be for as long as "the  
court deems appropriate." *Id.*

1 for the cell site information; however, the State argued that the order was the functional  
2 equivalent of a warrant. *Id.*

3 The Supreme Court rejected the State's argument. The Court held that while the  
4 cell cite order cites A.R.S. § 13-3016(C)(1) and (D)(1), which applies to warrants, the Court  
5 issued an order, not a warrant. *Id.* at 81. And a cell site order is based on a showing of  
6 reasonable grounds, not probable cause. *Id.* However, the Court upheld the denial of the  
7 motion to suppress because it found that the good-faith exception applied because the State  
8 reasonably relied on A.R.S. § 13-3016(C) which permitted the State to obtain cell site  
9 information without a warrant. *Id.*

10 The Court also rejected the defendant's argument that the cell site order was invalid  
11 because the State did not provide him with prior notice as is required by A.R.S. § 13-  
12 3016(B)(3). *Id.* at 82. The Court found that the defendant was wrong for two reasons.  
13 First, A.R.S. § 13-3016(D)(1) allows notice to be delayed for up to 90 days if the applicant  
14 requests a delay of notification for one or more of the reasons set forth in that statute. *Id.*  
15 The State requested delayed notice of the cell site order and the judge granted the request.  
16 *Id.* Second, the court found that the State timely disclosed the cell site information to the  
17 defendant within the 90 days permitted by A.R.S. § 13-3016(D)(1). *Id.*<sup>5</sup>

18 The defense argues that *Smith* demonstrates that A.R.S. § 13-3016 is the equivalent  
19 state statute to 18 U.S.C. § 2703(c). (Doc. 1267.) The defense points out that A.R.S. § 13-  
20 3016 requires that prior notice be provided to the subscriber or customer or that notice be  
21 delayed by the court when the government seeks to acquire cell site information by a court  
22 order. As a result, the defense argues that Section 2703(c) is less restrictive than A.R.S. §  
23 13-3016, because Section 2703(c)(3) allows the government to obtain a court order for cell  
24 site information without any notice to the subscriber. The defense represents that the  
25 defendants were never given prior notice as required by Section 13-3016; and the petitions

---

26  
27 <sup>5</sup> As discussed in text *infra*, contrary to the government's contention in their second  
28 supplemental pleading, *Smith* did not hold that suppression was not a remedy for a notice  
violation. Rather, the Arizona Supreme Court did not need to address that issue because it  
found that notice was lawfully delayed, and timely notice was ultimately provided.

1 did not seek delayed notification, and as a result, the orders did not authorize delayed  
2 notice. Because state law was violated, the defense argues that the government did not  
3 comply with the requirements of the SCA, and therefore, the good-faith exception does not  
4 apply.

5 The defense further points out that A.R.S. § 13-3016 applies to an “electronic  
6 communication,” and that term is defined as “any transfer of signs, *signals*, writing,  
7 images, sounds, *data or intelligence of any nature* that is transmitted in whole or in part by  
8 a wire, radio, electromagnetic, photoelectronic or photo-optical system[.]” (Doc. 1324 at  
9 4-5.) Thus, the defense contends that cell site information is included within “signals, data  
10 or intelligence of any nature that are transmitted,” and are thus covered by A.R.S. § 13-  
11 3016 which requires prior notice to the subscriber or customer, unless notice is lawfully  
12 delayed. *Id.* at 5. The defense reasons that the fact that A.R.S. § 13-3016 also applies to  
13 content, while Section 2703(c) does not, means only that A.R.S. § 13-3016 is more  
14 restrictive and provides subscribers and customers with greater protections. They claim  
15 that the Arizona Supreme Court recognized as much in *Smith*.

16 Finally, the defense argues that *Smith* precludes that government from arguing that  
17 the state court orders were the functional equivalent of a search warrant. And even if it  
18 could be viewed as such, Detective Padilla failed to follow established state search warrant  
19 procedures because the state judge’s order was not supported by an affidavit. *See* A.R.S.  
20 § 13-3914.<sup>6</sup>

21 The government argues that Section 13-3016 applies to contents of  
22 communications, and not cell site information. (Doc. 1271.) The government seems to  
23 argue that the officer who applied for cell site data in *Smith* cited the wrong Arizona statute,  
24 and that is why the court addressed A.R.S. § 13-3016. Specifically, the government states  
25 that in *Smith* the agent who submitted the application for cell site information cited to  
26 A.R.S. § 13-3016, so that court was forced to analyze that statute. The government

---

27  
28 <sup>6</sup> The government does not appear to make this argument given the Arizona Supreme Court’s finding in *Smith* that the order in that case was not the functional equivalent of a warrant.

1 maintains that the clear and unambiguous language of A.R.S. § 13-3016 states that it  
2 “applies to oral, wire and electronic communications that are entrusted to a communication  
3 service provider[.]” A.R.S. § 13-3106(A). As such, either A.R.S. § 13-3017 or A.R.S. §  
4 13-3018 is the Arizona equivalent to Section 2703(c) because they are the statutory  
5 authority for requests and orders for cell site information.

6 The Court notes that the government’s inability to make up its mind as to which  
7 Arizona statute applies to cell site information is telling. To be sure, the Arizona statutory  
8 scheme is not clear with respect to requests for cell site information, although frankly, the  
9 SCA is not a model of clarity. But the government’s position that cell site information can  
10 be obtained pursuant to both A.R.S. § 13-3017 and A.R.S. § 13-3018 shows their struggle  
11 to distinguish *Smith*, which specifically addressed a request for cell site information under  
12 A.R.S. § 13-3016. As discussed below, the Court concludes that, read in conjunction,  
13 *Conner*, *Mixton*, and *Smith* demonstrate that A.R.S. § 13-3016, and not A.R.S. § 13-3017  
14 or A.R.S. § 13-3018, is the state equivalent of Section 2703 for purposes of obtaining cell  
15 site information.

16 Again, A.R.S. § 13-3017 clearly does not apply to cell site information. That statute  
17 allows for the government to find out, using the phone numbers of a subscriber or customer,  
18 the calls or text messages made and received by the phone that is the subject of the pen/trap  
19 order, and not where the phone was located when calls or text messages were made or  
20 received.

21 Additionally, the Court cannot conclude that A.R.S. § 13-3018 applies to cell site  
22 information solely because the definition of “communication service records” in that  
23 statute includes “records of the path of an electronic communication between the point of  
24 origin and the point of delivery[.]” A.R.S. § 13-3018(G). The plain meaning of that portion  
25 of the definition of a “communication service record” is not clear from the statute itself.  
26 And, importantly, no court has addressed either this definitional section or A.R.S. § 13-  
27 3018 in terms of its applicability to cell site information. And *Mixton* only noted that  
28 A.R.S. § 13-3018 allows a prosecutor to subpoena IP addresses and subscriber information,



1 which *Carpenter* did not cast doubt on, and is not the issue here.<sup>7</sup>

2 The Court concludes that A.R.S. § 13-3016 is the state equivalent to Section 2703(c)  
3 based on *Smith* and the language (albeit not plain) of that statute. Again, in *Smith* the  
4 Arizona Supreme Court specifically addressed a request for cell site information made  
5 pursuant to A.R.S. § 13-3016 and held that the good-faith exception applied because the  
6 pre-*Carpenter* request for that information and resultant order complied with A.R.S. § 13-  
7 3016. *Smith* is the only Arizona case to specifically address the Arizona statute that applies  
8 to requests for cell site information. This Court must follow the only and highest authority  
9 on this issue governed by Arizona law.

10 Additionally, the Court finds that the definition of “electronic communication” for  
11 purposes of A.R.S. § 13-3016 supports that statute’s applicability to cell site information.  
12 Specifically, “electronic communication” includes “any transfer of signs, signals, writing,  
13 images, sounds, data or intelligence of any nature that is transmitted in whole or in part by  
14 a wire, radio, electromagnetic, photoelectronic, or photooptical system[.]” A.R.S. § 13-  
15 3001(4).<sup>8</sup> The references to the transfer of “signals, data, or intelligence of any nature”  
16 certainly seem to encompass cell site information, which is made up of signals, data, and/or  
17 intelligence of any nature. There is no doubt that the definition of “electronic  
18 communication” encompasses the content of communications. But that is not at all  
19 surprising since A.R.S. § 13-3016 allows the government to obtain the contents of  
20 communications (although only by a search warrant after *Carpenter*). The fact that A.R.S.  
21 § 13-3016 allows for content to be obtained does not foreclose this statute from also  
22 applying to requests for cell site information given the expansive definition of an  
23 “electronic communication.” Relatedly, the Court finds that “signals, data, or intelligence

24 <sup>7</sup> As the defense points out, even if A.R.S. § 13-3018 applied to requests for cell site  
25 information, Detective Padilla could not have used it if he wanted to because it requires a  
subpoena issued by a prosecutor.

26 <sup>8</sup> The Court notes that an “electronic communication” does not include any of the  
27 following: (a) any wire or oral communication; (b) any communication made through a  
28 tone-only paging device; or (c) any communication from a tracking device. A.R.S. § 13-  
3001(4). It is clear that these exceptions apply to the “real time” acquisition of that  
information.



1 of any nature” more aptly describes cell site information than “records of the path of an  
 2 electronic communication between the point of origin and the point of delivery,” which  
 3 A.R.S. § 13-3018 includes in its definition of a “communication service record.”<sup>9</sup>  
 4 Therefore, the Court concludes that A.R.S. § 13-3016’s expansive definition of “electronic  
 5 communications” also shows that this statute is the Arizona equivalent to Section 2703(c).

6 Finally, the Court finds that TPD’s practice in 2015 of obtaining court orders for  
 7 cell site information supports this Court’s conclusion that A.R.S. § 13-3016, and not A.R.S.  
 8 § 13-3018, is the Arizona equivalent of Section 2703(c). Detective Padilla testified he was  
 9 instructed by his superiors to obtain a court order for cell site information. As such, that  
 10 was his standard practice and the standard practice of the TPD in 2015, and apparently well  
 11 before 2015. That instruction was given and that practice was instituted even though the  
 12 government claims that A.R.S. § 13-3018 allows the State (albeit via the prosecutor) to  
 13 obtain historical cell site data by a subpoena that recited boilerplate language about the  
 14 investigative need for the cell site information. Detective Padilla never testified about why  
 15 he was instructed to obtain a court order for cell site information or why that was the  
 16 standard practice, rather than obtain a subpoena. He also did not testify about who gave  
 17 TPD what amounts to a legal opinion – *e.g.*, TPD counsel, the Pima County Attorney’s  
 18 Office, or the Attorney General’s office – which resulted in the instruction to obtain a court  
 19 order for this information. Thus, the only conclusion this Court can draw is that law  
 20 enforcement, and perhaps TPD counsel or state prosecutors, did not believe that historical  
 21 cell site information could lawfully be obtained by a subpoena under A.R.S. § 13-3018.

22 For the reasons stated above, the Court finds that A.R.S. § 13-3016 is the state  
 23 equivalent of Section 2703(c) for requesting a court order for cell site data. Both the  
 24 expansive definition of “electronic communication” for purposes of A.R.S. § 13-3016 and  
 25 the Arizona Supreme Court’s extensive discussion in *Smith* about A.R.S. § 13-3016’s  
 26 applicability to requests for cell site information, and the fact that content was not obtained

---

27 <sup>9</sup> The government certainly could have presented testimony from an employee of an  
 28 electronic communication service provider to opine on whether the cell site data is  
 encompassed within Section 13-3018’s definition of a “communication service record” or  
 Section 13-3016’s definition of “electronic communication.”

1 in that case, leaves little doubt in this Court's mind that A.R.S. § 13-3016 was the Arizona  
 2 counterpart to Section 2703(c) when the petitions were submitted to the state court in 2015.  
 3 The Court now turns to whether the government acquired cell site information in a manner  
 4 prohibited by Arizona State law.

5 Once again, Section 2703(d) provides that: "In the case of a State governmental  
 6 authority, such a court order shall not issue if prohibited by the law of such State." 18  
 7 U.S.C. § 2703(d). In 2015, Arizona law clearly did not have a blanket prohibition on the  
 8 government obtaining cell site information by a court order. To the contrary, the discussion  
 9 above demonstrates that A.R.S. § 13-3016 could be used to obtain a court order for cell  
 10 site information. However, unlike Section 2703(c), a court order for cell site information  
 11 could not issue under A.R.S. § 13-3016 unless: (a) prior notice is provided to the customer  
 12 or subscriber; or (b) court authorization to delay the notice for 90 days is obtained. Stated  
 13 another way, Section 13-3016 prohibits the acquisition of cell site information by a court  
 14 order if prior notice to the subscriber is not provided or delayed notice is not obtained.<sup>10</sup>

15 In the case at hand, the government's acquisition of cell site information was  
 16 prohibited under Section 13-3016 because prior notice was not provided to the customer  
 17 or subscriber and delayed notice was not obtained from the court. The government did not  
 18 present evidence that the defendants were provided with prior notice that the government  
 19 was obtaining their electronic communication records, or that notice was delayed. Defense

---

20 <sup>10</sup> The requirement that the government provide notice to subscribers or customers under  
 21 A.R.S. § 13-3016(G) regarding the acquisition of their "electronic communications" is not  
 22 ministerial or a technicality that law enforcement should be able to disregard without  
 23 consequence. Rather, the notification requirement serves an important purpose. A.R.S. §  
 24 13-3016(G) provides that upon expiration of the delayed notice, law enforcement must  
 25 deliver to the subscriber or party the process used to obtain the information and notice of  
 26 several things, including "[t]hat any challenge to the subpoena or order must be filed within  
 27 fourteen days." A.R.S. § 13-3106(G)(6). Subsection (G)(6) is essentially a procedural due  
 28 process provision in terms of advising a subscriber or party that they have the right to  
 challenge the subpoena or order, as well as advising them of the deadline by which they  
 must do so. The SCA has a counterpart to A.R.S. § 13-3106(G), specifically, 18 U.S.C. §  
 2705(a)(5). However, Section 2705(a)(5) does not require law enforcement to notify the  
 subscriber or customer that they have the right to challenge an order issued under the SCA.  
 And even if it did, the notification provision of Section 2705(a)(5) would not have applied  
 to the orders in the case at hand because Section 2703(c) does not require any notice to be  
 provided to the subscriber or customer. Thus, the notification provision of A.R.S. § 13-  
 3016 provides more protection to a subscriber or customer than the SCA.

1 counsel represented to the Court that both they and their clients learned about the  
2 acquisition of this information when counsel reviewed disclosure three years after the cell  
3 site orders were obtained. The petition submitted to the state judge never requested that  
4 law enforcement be authorized to delay notice to the subscriber or customer as is required  
5 under A.R.S. § 13-3016(B)(3); as a result, the judge's order did not authorize delayed  
6 notice.<sup>11</sup> The failure to provide prior notice or obtain an order for delayed notice resulted  
7 in the acquisition of cell site information in a manner prohibited under state law (*i.e.*, A.R.S.  
8 § 13-3016). As a result, the government did not comply with the then-lawful provisions of  
9 the SCA, specifically Section 2703(d), which is required to invoke the good-faith exception  
10 articulated in *Korte*.

11 Finally, the Court finds that there is another related reason why the government  
12 cannot rely on the good faith exception. That is, as the defense argues, Detective Padilla's  
13 "lackadaisical approach to the Petitions and Orders." (Doc. 1324 at 10.) Detective Padilla  
14 merely relied on forms provided by third-party communication service providers, which  
15 presumably serve every state, and simply filled in the blanks. As a result of the boilerplate  
16 forms, the petitions do not cite to any Federal or State statutory authority as the basis for  
17 the petitions, and the Orders that he prepared for the state judge (again, based on the forms  
18 provided to him), only cite to 18 U.S.C. § 2703 with no specification to the applicable  
19 subsection. *Id.*

20 The Court asked Detective Padilla to explain why he did not cite the statute that  
21 provides the legal basis to obtain the requested information. Tr. 3/14/22 (Doc. 1331) at 36-  
22 37. Detective Padilla testified that at the time, officers used "standard templates," so these  
23 petitions had been created using "a standard template that was brought or presented by the  
24 ZetX company to elicit what we needed." *Id.* at 37. Detective Padilla explained that the

---

25  
26 <sup>11</sup> The Court notes that the state judge included delayed notice language in his orders.  
27 However, the government acknowledges that the judge did not authorize law enforcement  
28 to delay notice to the subscriber; rather, the orders prohibited the cell phone companies  
from notifying the subscriber about the information provided to law enforcement.  
Assuming *arguendo* that the state court's order can be read to comply with the delayed  
notice requirements set forth in Section 13-3016(D), the order delayed notice indefinitely,  
and not for the 90-day period provided for in that statute.

1 companies that he was seeking the cell site information from provided him with what the  
 2 companies needed in the petitions and the orders to provide the requested information. *Id.*  
 3 The company drafted the templates for the petitions and orders, and officers would  
 4 download it from their website, fill it out, and “then print it as our final product and that  
 5 would be presented to the judge.” *Id.* at 37-38.

6 Detective Padilla certainly relied in good faith on the service providers. But, in  
 7 doing that, he demonstrated a careless disregard of whether these forms conformed to the  
 8 SCA or Arizona law. In fact, it is clear from Detective Padilla’s testimony that he had no  
 9 idea of the statutory authority being utilized to obtain the cell site information. His  
 10 complete deferral to the service providers, as opposed to TPD counsel or a prosecutor, also  
 11 forecloses the argument that he relied in good faith on the law to excuse this constitutional  
 12 violation.

13 **E. Suppression is a Remedy in the Case at Hand.**

14 The government argues that neither the SCA nor Arizona law provide for preclusion  
 15 of evidence as a remedy for a violation of either Section 2703(d) or state law (whether that  
 16 be A.R.S. §§ 13-3016, 13-3017, or 13-3018). Additionally, the government claims that the  
 17 Arizona Supreme Court in *Smith* held that violation of the notice provisions of A.R.S. §  
 18 13-3016 is not a basis for suppression. (Doc. 1317 at 8.)

19 The defense points out that Section 2708 states that “[t]he remedies and sanctions  
 20 described in this chapter are the only judicial remedies and sanctions for *nonconstitutional*  
 21 violations of this chapter.” (Doc. 1324 at 8; emphasis in original.) Thus, the fact that the  
 22 SCA does not provide for suppression of evidence as a remedy for the violation of that Act  
 23 is irrelevant to the instant motion because it is based on a constitutional challenge, which  
 24 includes the notice requirement set forth in A.R.S. § 13-3016.

25 Contrary to the government’s contention, the Arizona Supreme Court in *Smith*  
 26 never held or even intimated that suppression was not a remedy for a violation of the notice  
 27 requirements of A.R.S. § 13-3016. The Court did not have to address that issue because  
 28 it found that notice was initially lawfully delayed, and timely notice was ultimately

1 provided. Thus, *Smith* does not foreclose suppression as a remedy for the alleged  
2 constitutional violation in the case at hand.


3 The Court concludes that the defense is correct they are not limited to the remedies  
4 provided in the SCA. The defense presents a constitutional challenge to the state judge's  
5 orders under *Carpenter* because the government did not obtain a warrant. *Korte* provides  
6 a good-faith exception to that constitutional challenge that will defeat a motion to suppress  
7 if the government complied with the then-lawful SCA requirements. However, here, the  
8 government cannot establish that it complied with the then-lawful requirements of the  
9 SCA. As a result, *Korte*'s good-faith exception does not apply to excuse the constitutional  
10 violation. Because the state court's Section 2703 orders authorizing the acquisition of cell  
11 site data were unconstitutional, the fruits of the searches (that data) should be suppressed.

### 12 CONCLUSION

13 Accordingly, for the reasons stated above, the Court recommends that the District  
14 Court GRANT the motion to suppress.

15 Pursuant to Federal Rule of Criminal Procedure 59(b)(2), any party may serve and  
16 file written objections within 14 days of being served with a copy of this Report and  
17 Recommendation. A party may respond to the other party's objections within fourteen  
18 days. No reply brief shall be filed on objections unless leave is granted by the district court.  
19 If any objections are filed, this action should be designated case number: **CR 18-01695-**  
20 **TUC-JAS**. Failure to timely file objections to any factual or legal determination of the  
21 Magistrate Judge may be considered a waiver of a party's right to de novo consideration  
22 of the issues. See *United States v. Reyna-Tapia*, 328 F.3d 1114, 1121 (9th Cir. 2003) (en  
23 banc).

24 Dated this 8th day of July, 2022.

25   
26 \_\_\_\_\_  
27 Eric J. Markovich  
28 United States Magistrate Judge